UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/767,400	01/29/2004	Jeremy Mark Ellington		2874

7590 01/22/2008

Raymond M. Galasso
Simon, Galasson & Frantz PLC
P.O. Box 26503
Austin, TX 78755-0503

EXAMINER	
CHEN, SHIN HON	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
01/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/767,400	ELLINGTON, JEREMY MARK	
	Examiner	Art Unit	
	Shin-Hon Chen	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,8-13,15,16,19-24,27-32,34,35 and 38* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,8-13,15,16,19-24,27-32,34,35 and 38* is/are rejected.

7)☒ Claim(s) *1, 9, 20 and 28* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 January 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-5, 8-13, 15, 16, 19-24, 27-32, 34, 35 and 38 have been examined.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/14/07 has been entered.

Claim Objections

3. Claims 1, 9, 20 and 28 objected to because of the following informalities:

Regarding claim 1, "a computer system" in line 3 should be changed to "the computer system" because it is introduced in line 2 of claim 1.

Regarding claim 9, "a computer system" in line 3 should be changed to "the computer system" because it is introduced in line 2 of claim 9.

Regarding claim 20, "a computer system" in line 8 should be changed to "the computer system" because it is introduced in line 1 of claim 20.

Regarding claim 28, "a computer system" in line 8 should be changed to "the computer system" because it is introduced in line 1 of claim 28.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-5, 8-13, 15, 16, 19-24, 27-32, 34, 35 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bradee U.S. Pub. No. 20020095571 (hereinafter Bradee) in view of Kraus et al. U.S. Pub. No. 20030233571 (hereinafter Kraus).

6. As per claim 1, Bradee discloses a computer-implemented method for enabling users to access a computer system (Bradee: figure 3: computer systems 54A-54C), comprising:

authorizing access to a computer system by a user in response to determining authentication of at least one user via local authentication with respect to the computer system (Bradee: [0009] lines 13-15: authenticate the user based on user ID), wherein said authorizing access includes successfully verifying that the user has an active shared directory account associated with the computer system (Bradee: [0009] lines 15-18: reads data store to determine which surrogate id corresponds to the user's assigned role; [0009] lines 21-23: determine if the surrogate id is authorized to access secured resources);

selecting a universal local user account of the computer system dependent upon said shared directory account (Bradee: [0009] lines 15-18: determine which surrogate id corresponds to the user's assigned role),

wherein the universal local user account has access privilege on the computer system (Bradee: [0055] lines 1-5: surrogate id are used to determine access permissions); and

mapping the user to the universal local user account (Bradee: [0054] lines 1-3: associate user id with appropriate user role), wherein said mapping enables access to the computer system in accordance with an access privilege level corresponding to the universal local user account (Bradee: [0054]: associate surrogate ID to users).

Bradee discloses the user accesses enterprise computer system by normal log-in procedures (Bradee: [0038] lines 3-11: the user logs on the system and network through user id and password). Bradee does not explicitly disclose accessing the computer system as a remote user. However, Kraus discloses accessing a computer system through remote access and mapping the remote user id into local user id to determine access privilege (Kraus: [0068]: mapping remote user identifier to local user identity on the target system). It would have been obvious to one having ordinary skill in the art to allow the user to access multi-platform enterprise system resources through remote access because access of data through network is well known in the art and regardless whether access is achieved locally or remotely, the user id is mapped to a corresponding universal local user account as required by local authentication scheme. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Kraus within the system of Bradee because remote access allows a user to centrally manage/access servers in different platforms (Kraus: [0008]).

7. As per claim 2, Bradee as modified discloses the method of claim 1. Bradee further discloses wherein selecting the universal local user account of the computer system dependent

upon said shared directory account includes determining at least one of directory services group membership information associated with said shared directory account and access privilege information associated with said shared directory account (Bradee: [0042] lines 1-3: retrieves from a data store, a surrogate ID and password corresponds to user's assigned role; [0053]: user roles specify access privileges).

8. As per claim 3, Bradee as modified discloses the method of claim 1. Bradee as modified further discloses wherein said selecting the universal user account includes correlating a universal local user account access level to a corresponding group membership of the remote user (Bradee: [0054] lines 6-10: surrogate ID represent all those who have a particular user role; [0055] lines 1-3: permissions are associated with each particular surrogate ID).

9. As per claim 4, Bradee as modified discloses the method of claim 1. Bradee further discloses wherein the universal local user account is one of a plurality of universal local user accounts (Bradee: [0053]: privileges are grouped together under a specific user role); and each one of said universal local user accounts has a respective access privilege level associated therewith (Bradee: [0054] lines 1-3: associate users with user roles).

10. As per claim 5, Bradee as modified discloses the method of claim 1. Bradee further discloses creating said plurality of universal local user accounts prior to performing said selecting, wherein each one of said universal local user access accounts has a respective access

privilege level associated therewith (Bradee: [0009] lines 15-18: if authentication is successful, determine which surrogate id corresponds to user's assigned role).

11. As per claim 8, Bradee as modified discloses the method of claim 1. Bradee as modified further discloses wherein several users can be simultaneously mapped to the universal local user account for enabling simultaneous access by each one of said remote users to the computer system (Bradee: [0024] lines 1-3: simultaneously call the security module for authentication).

12. As per claim 9, Bradee discloses a computer-implemented method for enabling users to access a computer system (Bradee: figure 3: computer systems 54A-54C), comprising:

determining that a user of a computer system is an authenticated user via local authentication with respect to the computer system (Bradee: [0009] lines 13-15: authenticate the user based on user ID); and

associating the user with a universal local user account after said determining (Bradee: [0009] lines 15-18: if authentication is successful associate user id with surrogate id/universal local account) and after determining that the user has an active shared directory account associated with the computer system (Bradee: [0009] lines 16-17: determine which surrogate id corresponds to user), wherein the universal local user account has access privilege on the computer system (Bradee: [0057] lines 1-4: user roles are system-wide set of application permissions) and wherein said associating enables access to the computer system in accordance with said access privilege corresponding to the universal local user account (Bradee: [0047] lines 1-6: subsequent access requests are granted or denied based on the surrogate id).

Bradee discloses the user accesses enterprise computer system by normal log-in procedures (Bradee: [0038] lines 3-11: the user logs on the system and network through user id and password). Bradee does not explicitly disclose accessing the computer system as a remote user. However, Kraus discloses accessing a computer system through remote access and mapping the remote user id into local user id to determine access privilege (Kraus: [0068]: mapping remote user identifier to local user identity on the target system). It would have been obvious to one having ordinary skill in the art to allow the user to access multi-platform enterprise system resources through remote access because access of data through network is well known in the art and regardless whether access is achieved locally or remotely, the user id is mapped to a corresponding universal local user account as required by local authentication scheme. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Kraus within the system of Bradee because remote access allows a user to centrally manage/access servers in different platforms (Kraus: [0008]).

13. As per claim 10, Bradee as modified discloses the method of claim 9. Bradee as modified further discloses wherein associating the remote user with the universal local user account includes determining at least one of directory services group membership information associated with said shared directory account (Bradee: [0053]: user roles are defined based on job functions and privileges required to perform certain tasks).

14. As per claim 11, Bradee as modified discloses the method of claim 9. Bradee as modified further discloses wherein said associating includes correlating a universal local user account

access level to a corresponding access level of a group membership of the remote user (Bradee: [0057]: user role is system-wide set of application permissions that defines privileges of users who have the same job responsibilities).

15. As per claim 12, Bradee as modified discloses the method of claim 9. Bradee further discloses wherein the universal local user account is one of a plurality of universal local user accounts (Bradee: [0053]: user roles); and each one of said universal local user accounts has a respective access privilege level associated therewith (Bradee: [0052]: specify certain privilege for certain group of users).

16. As per claim 13, Bradee as modified discloses the method of claim 9. Bradee further discloses creating said plurality of universal local user accounts prior to performing said selecting, wherein each one of said universal local user access accounts has a respective access privilege level associated therewith (Bradee: [0053]: define user roles by grouping access privileges based on needs and functions required).

17. As per claim 15, Bradee as modified discloses the method of claim 14. Bradee further discloses wherein said user account selection information includes at least one of directory services group membership information and access privilege information (Bradee: [0054] lines 1-3: associate user IDs with appropriate user roles in the data store).

18. As per claim 16, Bradee as modified discloses the method of claim 14. Bradee as modified further discloses wherein said selecting the universal user account includes correlating a universal local user account access level to an access level of a group membership of the remote user (Bradee: [0053]: privileges are associated with each user role).

19. As per claim 19, Bradee as modified discloses the method of claim 9. Bradee as modified further discloses wherein several users can be simultaneously mapped to the universal local user account for enabling simultaneous access by each one of said remote users to the computer system (Bradee: [0024] lines 1-3: simultaneously call the security module to authenticate users).

20. As per claim 20, Bradee discloses a computer system, comprising:

at least one data processing device (Bradee: figure 3: computers 54A-54C are data processing devices);

instructions processable by said at least one data processing device (Bradee: [0009] lines 1-4: embedded software applications); and

an apparatus from which said instructions are accessible by said at least one data processing device (Bradee: [0009] lines 2: securing resources stored on the computer system);

wherein said instructions are configured for enabling said at least one data processing device to facilitate:

authorizing access to the computer system by a user in response to determining the user is authenticated user via local authentication with respect to the computer system (Bradee: [0009] lines 13-15: authenticate the user based on user ID), wherein said

authorizing access includes successfully verifying that the remote user has an active shared directory account associated with the computer system (Bradee: [0009] lines 15-18: reads data store to determine which surrogate id corresponds to the user's assigned role; [0009] lines 21-23: determine if the surrogate id is authorized to access secured resources);

selecting a universal local user account of the computer system dependent upon said shared directory account (Bradee: [0009] lines 15-18: determine which surrogate id corresponds to the user's assigned role),

wherein the universal local user account has access privilege on the computer system (Bradee: [0055] lines 1-5: surrogate id are used to determine access permissions); and

mapping the user to the universal local user account (Bradee: [0054] lines 1-3: associate user id with appropriate user role), wherein said mapping enables access to the computer system in accordance with an access privilege level corresponding to the universal local user account (Bradee: [0054]: associate surrogate ID to users based on user roles).

Bradee discloses the user accesses enterprise computer system by normal log-in procedures (Bradee: [0038] lines 3-11: the user logs on the system and network through user id and password). Bradee does not explicitly disclose accessing the computer system as a remote user. However, Kraus discloses accessing a computer system through remote access and mapping the remote user id into local user id to determine access privilege (Kraus: [0068]: mapping remote user identifier to local user identity on the target system). It would have been obvious to one having ordinary skill in the art to allow the user to access multi-platform

enterprise system resources through remote access because access of data through network is well known in the art and regardless whether access is achieved locally or remotely, the user id is mapped to a corresponding universal local user account as required by local authentication scheme. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Kraus within the system of Bradee because remote access allows a user to centrally manage/access servers in different platforms (Kraus: [0008]).

21. As per claim 21, Bradee as modified discloses the computer system of claim 20. Bradee further discloses wherein selecting the universal local user account of the computer system dependent upon said shared directory account includes determining at least one of directory services group membership information associated with said shared directory account and access privilege information associated with said shared directory account (Bradee: [0042] lines 1-3: retrieves from a data store, a surrogate ID and password corresponds to user's assigned role; [0053]: user roles specify access privileges).

22. As per claim 22, Bradee as modified discloses the computer system of claim 20. Bradee as modified further discloses wherein said selecting the universal user account includes correlating a universal local user account access level to a corresponding group membership of the remote user (Bradee: [0054] lines 6-10: surrogate ID represent all those who have a particular user role; [0055] lines 1-3: permissions are associated with each particular surrogate ID).

23. As per claim 23, Bradee as modified discloses the computer system of claim 20. Bradee further discloses wherein the universal local user account is one of a plurality of universal local user accounts (Bradee: [0053]: privileges are grouped together under a specific user role); and each one of said universal local user accounts has a respective access privilege level associated therewith (Bradee: [0054] lines 1-3: associate users with user roles).

24. As per claim 24, Bradee as modified discloses the computer system of claim 20. Bradee further discloses creating said plurality of universal local user accounts prior to performing said selecting, wherein each one of said universal local user access accounts has a respective access privilege level associated therewith (Bradee: [0009] lines 15-18: if authentication is successful, determine which surrogate id corresponds to user's assigned role).

25. As per claim 27, Bradee as modified discloses the computer system of claim 20. Bradee as modified further discloses wherein several users can be simultaneously mapped to the universal local user account for enabling simultaneous access by each one of said remote users to the computer system (Bradee: [0054] lines 7-11: surrogate ID represents all users with same privilege).

26. As per claim 28, Bradee discloses a computer system, comprising:

at least one data processing device (Bradee: figure 3: computers 54A-54C are data processing devices);

instructions processable by said at least one data processing device (Bradee: [0009] lines 1-4: embedded software applications); and

an apparatus from which said instructions are accessible by said at least one data processing device (Bradee: [0009] lines 2: securing resources stored on the computer system);

wherein said instructions are configured for enabling said at least one data processing device to facilitate:

determining that a user of a computer system is an authenticated user via local authentication with respect to the computer system (Bradee: [0009] lines 13-15: authenticate the user based on user ID); and

associating the user with a universal local user account after said determining (Bradee: [0009] lines15-18: if authentication is successful associate user id with surrogate id/universal local account) and after determining that the user has an active shared directory account associated with the computer system (Bradee: [0009] lines 16-17: determine which surrogate id corresponds to user), wherein the universal local user account has access privilege on the computer system (Bradee: [0057] lines 1-4: user roles are system-wide set of application permissions) and wherein said associating enables access to the computer system in accordance with said access privilege corresponding to the universal local user account (Bradee: [0047] lines 1-6: subsequent access requests are granted or denied based on the surrogate id).

Bradee discloses the user accesses enterprise computer system by normal log-in procedures (Bradee: [0038] lines 3-11: the user logs on the system and network through user id and password). Bradee does not explicitly disclose accessing the computer system as a remote

user. However, Kraus discloses accessing a computer system through remote access and mapping the remote user id into local user id to determine access privilege (Kraus: [0068]: mapping remote user identifier to local user identity on the target system). It would have been obvious to one having ordinary skill in the art to allow the user to access multi-platform enterprise system resources through remote access because access of data through network is well known in the art and regardless whether access is achieved locally or remotely, the user id is mapped to a corresponding universal local user account as required by local authentication scheme. Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Kraus within the system of Bradee because remote access allows a user to centrally manage/access servers in different platforms (Kraus: [0008]).

27. As per claim 29, Bradee as modified discloses the computer system of claim 28. Bradee as modified further discloses wherein associating the remote user with the universal local user account includes determining at least one of directory services group membership information associated with said shared directory account (Bradee: [0053]: user roles are defined based on job functions and privileges required to perform certain tasks).

28. As per claim 30, Bradee as modified discloses the computer system of claim 28. Bradee as modified further discloses wherein said associating includes correlating a universal local user account access level to a corresponding access level of a group membership of the remote user (Bradee: [0057]: user role is system-wide set of application permissions that defines privileges of users who have the same job responsibilities).

29. As per claim 31, Bradee as modified discloses the computer system of claim 28. Bradee further discloses wherein the universal local user account is one of a plurality of universal local user accounts (Bradee: [0053]: user roles); and each one of said universal local user accounts has a respective access privilege level associated therewith (Bradee: [0052]: specify certain privilege for certain group of users).

30. As per claim 32, Bradee as modified discloses the computer system of claim 28. Bradee further discloses wherein said instructions are further configured for enabling said at least one data processing device to facilitate: creating said plurality of universal local user accounts prior to performing said selecting, wherein each one of said universal local user access accounts has a respective access privilege level associated therewith (Bradee: [0053]: define user roles by grouping access privileges based on needs and functions required).

31. As per claim 34, Bradee as modified discloses the computer system of claim 32. Bradee further discloses wherein said user account selection information includes at least one of directory services group membership information and access privilege information (Bradee: [0054] lines 1-3: associate user IDs with appropriate user roles in the data store).

32. As per claim 35, Bradee as modified discloses the computer system of claim 32. Bradee as modified further discloses wherein said selecting the universal user account includes

correlating a universal local user account access level to an access level of a group membership of the remote user (Bradee: [0053]: privileges are associated with each user role).

33. As per claim 38, Bradee as modified discloses the computer system of claim 28. Bradee as modified further discloses wherein several remote users can be simultaneously mapped to the universal local user account for enabling simultaneous access by each one of said remote users to the computer system (Bradee: [0024] lines 1-3: simultaneously call the security module to authenticate users).

Response to Arguments

34. Applicant's arguments with respect to claims 1-5, 8-13, 15, 16, 19-24, 27-32, 34, 35 and 38 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

35. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Blanco et al. U.S. Pat. No. 6539482 discloses network access authentication system based on remote and standard password.

Somin et al. U.S. Pub. No. 20050044411 discloses peer-to-peer authorization method utilizing remote access authentication.

Nukui U.S. Pat. No. 5239648 discloses computer network capable of accessing file remotely between computer systems.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Examiner
Art Unit 2131